Evaluating the Security Risks of the Modern Patient Experience

Sean Mehner, Connecticut Information Security

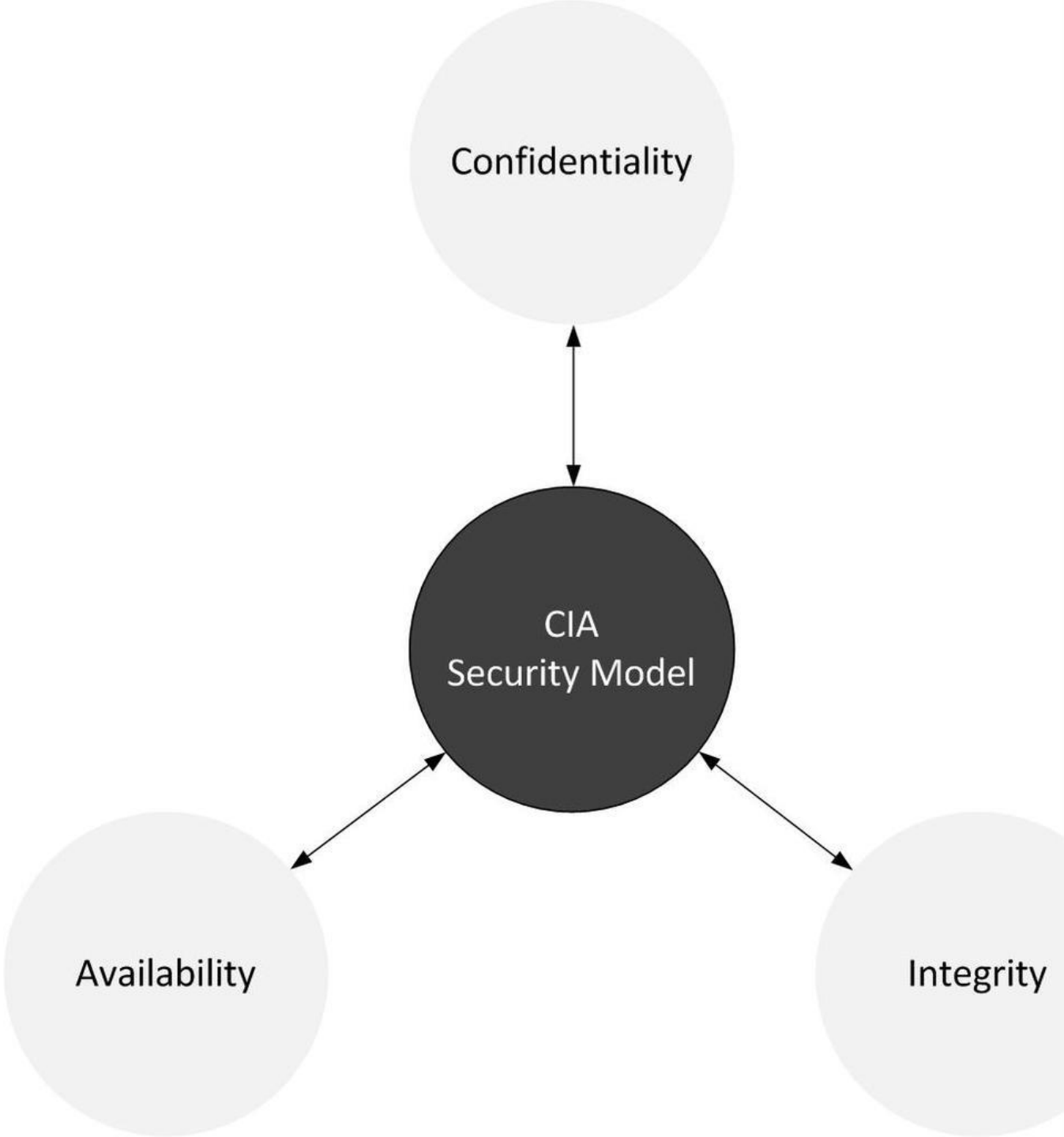
May 17, 2019

Sean Mehner

- Principal, Connecticut Information Security
- Partners with organizations to understand their unique security exposures and mitigate their risks.
- 20 years building the IT and security frameworks for many of today's largest organizations, including a great deal in healthcare.
- Recognized leader in security risk assessment, as well as technical testing such as web application and network penetration testing.
- Certified Information Systems Security Professional (CISSP), a Certified Information Systems Auditor (CISA) and a HealthCare Information Security and Privacy Practitioner (HCISPP).

Our Objectives Today

- Explore the future of cybersecurity for highly customizable and interactive patient experiences.
- Understand the unique cybersecurity risks and challenges that bringing automation and building controls into your patient environment pose.
- Learn strategies to reduce risk while continuing to provide rich patient experiences.



What do we need to know?

- Where has the landscape changed for the patient, and what can they expect going forward?
- What are some of the new exposures and touch points created through these offerings?
- How do these scenarios increase or create new risks?
- What can be done to limit your exposures without sacrificing patient care?

Evolving Patient Experience

- Changing very rapidly from even a few years ago; patients are starting to expect this.
- Guest Wi-Fi was originally seen as a great value add.
- The use of public kiosks and shared tablets became increasingly popular.
- Online portals for check out, pharmacy orders, and medical records access began to grow, along with biometric authentication for services, medicine, and access controls.

Evolving Patient Experience (cont.)

- Today we see remote monitoring of the patient with:
  - real-time alerts,
  - mobile self care platforms
  - telemedicine for both in and outpatient solutions
  - virtual operating room collaborations
  - very customized patient experiences the follow patients through a hospital
- Patients have more control of their experience including direct access to BMS controls through software.
- Remotely managed vendor devices, such as robots, have interfaces into elevators banks controllable from anywhere.
- Voice devices that tie into these traditionally isolated environments are sending speech to the cloud for processing.

Growth is complex

- **Providing guest Wi-Fi for overnight guests was easy. Today not so much.**
  - Shared resources
  - Not always decoupled from corporate solutions
  - Moving to cloud management
  - Limited accountability
- **Everything is becoming mobile.**
  - Blurred lines of internal and external offerings (vendor handoffs are not always clear)
  - Private cloud services are rolled into ‘internal’ solutions requiring more access into secured environments
- **We have the experience at home.**
  - Personalized temperature controls
  - Voice integrations
  - Remote cameras
- **Combining unlike resource types.**
  - Data is in many locations, and control points are expanding, making monitoring and tracking difficult
  - Solutions are starting to co-mingle secure and insecure systems (Video and medical records)

Too Much Exposure

Blending traditionally protected solutions with minimal authorization is dangerous.

HVAC / Lighting / Power / Elevator Controls / Cameras

Allowing loosely controlled remote access for critical systems

Giving unrestricted Internet access on hospital assets to a patient is also dangerous, worse if that device has access to internal resources.

Support is becoming more complex as well. Multiple teams and resources are needed to support various components of a solution. It is not always clear who owns what.

Forget Stuxnet. Malware already exists to target BAS environments with numerous proof of concept attacks against various systems.

Nation state technology and research is not needed.

Combine this with shared controls and the risks of an issue increase dramatically.

The ‘smarter’ the building the bigger the risks.

Taking Down Traditional Barriers

- Secure, cheap, and fast; pick any two.
- It is often more cost effective to leverage existing infrastructure than it is to build new.
  - Is the cost of separation worth it?
- Relying more and more on cloud infrastructure and hybrid models.
  - Allowing a vendor to manage or partially manage solutions is expanding the exposures.
- Solutions are built faster than they can be properly evaluated. Accepted risks are growing inside organizations and many are siloed (Big bubble exists in healthcare)

What's Happening Today?
Real World Scenarios

Scenario #1

- External facilities management system in place to support hospital BMS environment. Phishing attack targeted at the vendor.

Stolen credentials

Scenario #2

- Patient portal that integrates personalized controls, entertainment, and medical tracking within a patient room are deployed via tablets. Tablets allow browsing to the internet.

Patient portal tampering

Scenario #3

- Patient rooms are equipped with camera systems for safety monitoring. Cameras are deployed with limited security controls including default passwords for viewing.

Unauthorized viewing

No Shortage of Concerns

- In addition to these brief scenarios, many more real life examples
- Operating rooms systems are being shared via Internet for collaboration purposes
- Many older systems and solutions support the monitoring, access, and automation of critical environments
- Attacks are no longer one to one, meaning, there are many more targets at risk to the same thing
- Very limited monitoring of BMS solutions. For example failed logins or malformed requests
- The protection of isolation is disappearing

How do we make this better?

RNA

The stock answer is isolation, but the better answer is RNA (Risk Based Access Control)

DevSecOps

Gaining in popularity, but not everyone is ready for this

Nail the basics

Don’t look beyond a good core and strong fundamentals (patching, passwords, inventory)

Strong monitoring

If you can’t beat them, catch them

Access Control

Presentation Layer

- It is recommended limit links or functionality that is not accessible to a user. The purpose is to minimize unnecessary access control messages and minimize privileged information from being unnecessarily provided to users.

Business Layer

- Ensure that an access control verification is performed before an action is executed within the system.

Data Layer

- Ensure that an access control verification is performed to check that the user is authorized to act upon the target data. Do not assume that a user authorized to perform action X is able to necessarily perform this action on all data sets.

Better Risk Evaluation

- Don’t just go by the CVSS, vendor, or scanner scores. A CVSS of 0 in the wrong situation can be a considerable risk.
- Determine who might have access, and consider the risks those environments bring.
- Define exposure and exploitability. If something has no exposures it will be difficult to exploit.
- Involve security intel in guiding risk determination. Is the finding public or private? Does it require user interaction, is there proof of concept code?


QUESTIONS?